WHAT IS CLAIMED IS:

1. An originality guarantee system, comprising:

an embedded information apparatus which embeds information into a plurality of structural data

comprises:

and includes a data standardization device that sorts the plurality of structural data on the basis of a first rule, a message digest generation device that calculates a message digest with a predetermined hash function, for a bit stream composed of the plurality of structural data sorted by the data standardization device, and a data transformation that sorts the plurality of structural data sorted by the device data standardization device, on the basis of a second rule that is different from the first rule, with a key being the message digest calculated by said message digest generation device; and

an information alteration detection apparatus which detects any alteration of the plurality of structural data with the information that is embedded by the embedded information apparatus including a data standardization device that sorts a plurality of structural data on the basis of the first rule, a message digest generation device that calculates a message digest with the hash function, for a bit stream composed of the plurality of structural data that is sorted by said data standardization device a data transformation device that sorts the plurality of structural data sorted by said data standardization device on the basis of the second rule, with a key being the message digest calculated by said message digest generation device and

a decision device that compares the plurality of structural data, which is sorted by said data transformation device, with the plurality of structural data before being sorted by said data standardization device, and that decides the plurality of structural data, before being sorted by said data standardization device, have not been altered when both of the structural data match, and decides the plurality of structural data, before being sorted by said data standardization means, have been altered when both of the structural data do not match.

2. An embedded information apparatus, comprising:

a data standardization device that sorts a plurality of structural data on the basis of a predetermined rule;

message digest generation device that calculates a message digest with a predetermined hash function, for a bit stream composed of the plurality of structural data sorted by said data standardization device; and

data transformation device that sorts the plurality of structural data sorted by said data standardization device, on the basis of a rule that is different from the first-mentioned rule, with a key being the message digest calculated by said message digest generation device.

3. An information alteration detection apparatus, comprising:

data standardization device that sorts a plurality of structural data on the basis of a first rule being the same as that of data standardization device of an embedded information apparatus;

message digest generation device that calculates a message digest with a predetermined hash function, for a bit stream composed of the plurality of structural data sorted by said data standardization device;

a data transformation device that sorts the plurality of structural data sorted by said data standardization device, on the basis of a rule being that is different from the first rule and is the same as that of data transformation device of the embedded information apparatus, with a key being the message digest calculated by said message digest generation device; and

a decision device that compares the plurality of structural data sorted by said data transformation device with the plurality of structural data before being sorted by said data standardization device, and that decides the plurality of structural data, before being sorted by said data standardization device, have not been altered when both of the structural data match, and decides the plurality of structural data, before being sorted by said data standardization device, have been altered when both of the structural data do not match.

4. An embedded information method, comprising:

sorting a plurality of structural data on the basis of a first rule;

calculating a message digest with a predetermined hash function, for a bit stream composed of the plurality of sorted structural data; and

sorting the plurality of sorted structural data on the basis of a second rule that is different from the first rule by using the calculated message digest as a key.

5. An information alteration detection method, comprising:

sorting a plurality of structural data on the basis of the first rule in the embedded information method as defined in claim 4;

calculating a message digest with a predetermined hash function, for a bit stream composed of the plurality of sorted structural data;

sorting the plurality of sorted structural data on the basis of the second rule in the embedded information method by using the calculated message digest as a key; and

comparing the plurality of structural data, which is sorted on the basis of the second rule, with the plurality of structural data, before being sorted on the basis of the first rule, and deciding the plurality of structural data, before being sorted on the basis of the first rule, have not been altered when both of the structural data match, and deciding the plurality of structural data, before being sorted on the basis of the first rule, have been altered when both of the structural data do not match.

6. A computer-readable record medium that stores and executes an embedded information program on a computer, comprising:

sorting a plurality of structural data on the basis of a first rule;

calculating a message digest with a predetermined hash function, for a bit stream composed of the plurality of sorted structural data; and

sorting the plurality of sorted structural data on the basis of a second rule that is different from the first rule by using the calculated message digest as a key.

7. A computer-readable record medium that stores and executes an information alteration detection program on a computer, comprising:

sorting a plurality of structural data on the basis of the first rule in the sorting process which proceeds in such a way that the computer runs the embedded information program as defined in claim 6;

calculating a message digest with a predetermined hash function, for a bit stream composed of the plurality of sorted structural data;

sorting the plurality of sorted structural data on the basis of the second rule in said embedded information method by using the calculated message digest as a key; and

comparing the plurality of structural data, which is sorted on the basis of the second rule, with the plurality of structural data, before being sorted on the basis of the first rule, and deciding the plurality of structural data, before being sorted on the basis of the first rule, have not been altered when both of the structural data match, and deciding the plurality of structural data, before being sorted on the basis of the first rule, have been altered when both of the structural data do not match.